Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 1078-1081
doi:10.4028/www.scientific.net/AEF.6-7.1078

A Simulation Platform for Quantum Key Distribution Protocol

Zhu Lijuan

Information Technology dept. Shanghai JianQiao College , Shanghai China, 201319

zhulijuan@tokind.com.cn

Keywords: quantum key distribution protocol simulation, .NET, C#, BB84

Abstract. Quantum key distribution protocol is a hot spot of research in the information security, so, lots of Quantum key distribution protocol appeared. Every quantum protocol needs to be confirmed whether it is feasible and safe, if all those quantum protocols use physics experiment to verify, it is very complex and expensive. So, we introduce the platform, a functional platform for quantum key distribution protocols simulation. This platform introduces communication receiver, sender, establishment and protocol selection etc and it was designed on .NET IDE, the main programming language is C#. We simulated the existing BB84 protocol on this platform, and got the simulation results which were completely tallied with theoretic results.

Introduction

In 1985, David proposed quantum Turing machine model, and emerged the concept of quantum computer. In 1995, Peter Shor put forward the shor's quantum algorithm which can decompose a large prime numbers very quickly [1], so cryptography based on math will be deciphered. Quantum cryptography based on the principles of quantum mechanics is the only choice to solve that problem, so to find a secure key distribution algorithm has become a new research hotspot [2]. With the success of the quantum key distribution algorithm [3], people began to study quantum key distribution protocol.

Since BB84 protocol in 1984 and B92 protocol in 1992 and EPR protocol in 1993 were presented, researchers from all over the world had proposed many improved protocols or new protocols based on those three protocols. These research methods about these protocols have two kinds: one is theory and the other is experiment. Because of the physical characteristics of quantum state, it is very difficult to produce and preserve quantum state in the laboratory, and it is also very complex and expensive to measure these quantum state produced, and only some standard quantum key distribution protocol had been verified through the experiment, and many proposed quantum key distribution protocols were proved mainly by theoretical argument [4]. Even if it is purely theoretical analysis, a large number of complex mathematical derivations must be used. Therefore, the author designed and implemented a quantum key distribution protocol simulation platform on C# .Net platform and simulated the BB84 protocol on it, and it was exciting to find the simulation results consistent with the experiment results.

Simulation Platform Design Plan

Simulation platform was designed based on the object oriented development methods, and every main module of the platform in software was a separate project, and it could be packaged into a DLL file reused efficiently.

Demand Analysis. According to demand analysis, the simulation platform can simulate quantum key distribution protocol in the classic computer. When the program is running, the user can directly interact with the simulation platform, and implement distribution simulation under the condition of quantum key protocol state set up. At the same time, the user can see result of each step of the communication through the visualization window.

Overall Design. Using the idea of object-oriented programming, we divided the simulation platform into three layers: the first layer is to establish communication layer, which is the bottom of simulation platform; the second layer is a key transport layer; the third layer is access layer of security key. The logical control structure of three layers is shown in Fig. 1.

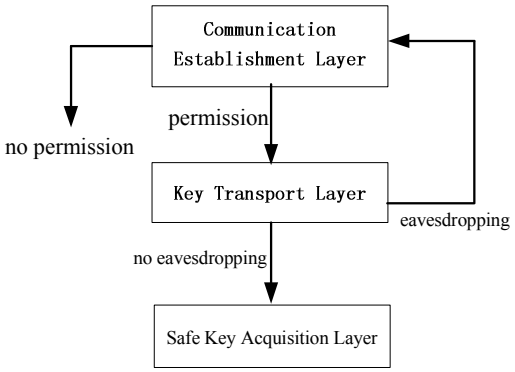

Fig. 1 The logical control structure among three layers

Communication Establishment Layer. Communication establishment layer is mainly composed of three modules, and they are " sender", "receiver" and "communication establishment". The sender is represented by Alice, and The receiver is represented by Bob. Communication establishment layer is shown in Fig. 2.

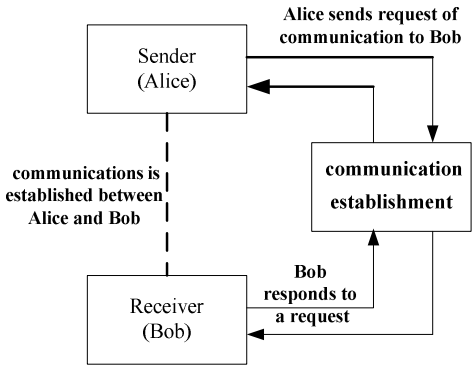

Fig. 2 Communication establishment layer

As Fig .2 shows, Alice calls "communication establishment" module and sends a communication request to Bob, and after Bob receives Alice's request, he also calls "communication establishment" module and responses Alice's request. When they set up communications, their communications enter the key transmission layer.

Key Transport Layer. After communication is established between Alice and Bob in "communication establishment" module, their next communication begins in the key transmission layer which is the most important layer of three layers. This layer includes "protocol selection" module, "quantum preparation" module and etc. The key transport layer is shown in Fig. 3.

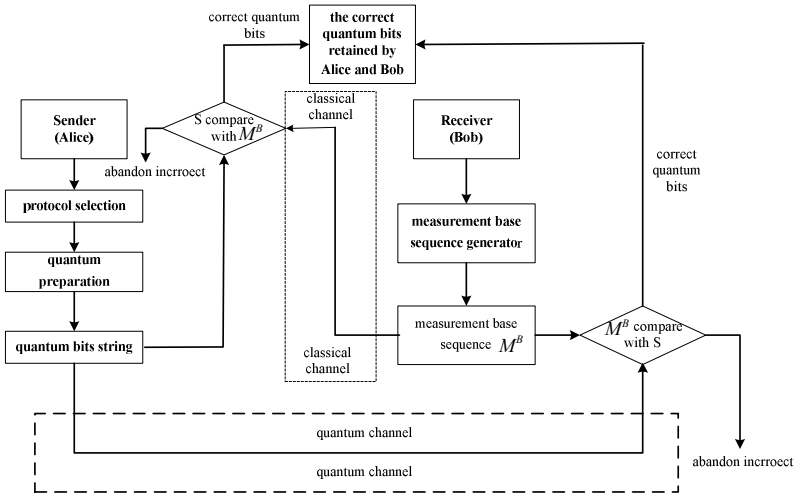

Fig. 3 Key transport layer

In the key transport layer, Alice calls "protocol selection" module to select protocol, and "quantum preparation" module prepare quantum bit S according to the selected protocol. After Bob calls "measurement base sequence generator" module to prepare a random measurement base sequence and sends this base sequence to the Alice, he compared it with S from Alice. At the same time, Alice makes a comparison between the base sequence received from Bob and S. Finally, they both retain the correct quantum bits, and then their communications enter the safe key acquisition layer.

Safe Key Acquisition. As Fig. 3 shows, if noise or eavesdropping is put into quantum channel, quantum bit deflection error must be corrected by using quantum error correction code CSS [4, 5], and the purpose is to avoid the noise error for eavesdropping and loss of a key acquisition. First, ξ_0 make the threshold of the bit error rate, and if $\xi \le \xi_0$, both sides continue to communicate, or stop communicating.

Simulation Platform Validation

BB84 protocol is verified by Windows based on cooperation of each module. Simulation interface is shown in Fig. 4.

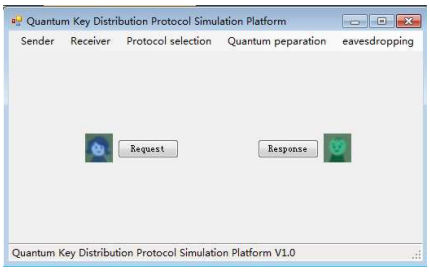

Fig. 4 Visual simulation of the main interface

The simulation process is as follows:

First, Alice sends a communication request to Bob，and Bob makes a response. If Bob agrees to Alice’s communication request, communication is established between them.

Second, Alice calls "BB84 protocol" module, and then quantum channel and classical channel are established.

Third, Alice calls "BB84 protocol _ photon generator" of " Quantum preparation" module, and this module will produce quantum bit string randomly {|↔>, |↕>, |↙>, |↕>, |↘>, |↕>, |↔>, |↙>, |↘>, |↕>} and this string is send to Bob through the quantum channel.

Fourth, After Bob receives the quantum bit string, he choices measurement base sequence{⊥， ⊥ , ○, ⊥, ⊥, ⊥, ○, ○, ○, ○} from "measurement base sequence generator" randomly to measure, and finally gets {？ , |↕>, |↙>, |↕>, ？ , |↕>, ?, |↙>, |↘>, ？ }.

Fifth, Before Bob measures a quantum bit string from Alice, he must send measurement base sequence selected from "measurement base sequence generator" randomly to Alice through the classical channel. Alice receives it, and then compares it with her own quantum bit string, and sends the comparison result {×, √, √, √, ×, √, ×, √, √, ×} to Bob through the classical channel.

Finally, Alice and Bob save the same measurement result {|↕>, |↙>, |↕>, |↕>, |↙>, |↖>}, and encode it into binary bits {101101} according to an agreement retained by them before, and the binary bits {101101} is the primary key. At this time, we make use of secure strengthening technology to process primary further in order to obtain a more secure key.

If eavesdropping is put into sequence (3) mentioned up, quantum bits Alice sent will be deflected. Bob makes a comparison between the measurement results and the returned results from (5) mentioned up, and uses quantum error correcting code CSS to correct that result. If error rate of that result exceeds predetermined error rate, Bob will abandon this key, otherwise reserve this key.

Compared with the theoretical results from BB84 protocol, the result obtained from the simulation platform is consistent with it in numerical terms and the simulation platform is further proved to be correct and practical.

Summary

Depends on the quantum state of the two different characteristics, quantum key distribution have two main types of protocols [2], one kind is single particle key distribution protocol based on non-orthogonal quantum state can not be cloned, and the other kind is key distribution protocol based on quantum entanglement properties. The author realized the first type of protocol simulation on the quantum simulation platform, and how to make the platform versatility is the subject of further study.

References

[1] Shor P W, Algorithms for quantum computation: discrete logarithms and factoring, 35 Annual Symposium on the Foundation of Computer Science, Proceeding, IEEE Computer Society Press, 1994.

[2] Zhao Sheng-mei, Li Fei, Zheng Bao-yu, Simulation of quantum key distribution on classical computer, Chinese Journal of Quantum Electronics. 3 (2004) 331-336.

[3] Bennett C H, Bessette F, Brassard G,et a1, Experimental quantum cryptography, Journal of Cryptology. 5 (1992) 3-28.

[4] Calderbank A R, Shor P W, Good quantum error correcting codes exist, Phys. Rev. A. 54 (1996) 1098-1105.

[5] Steane A M, Multiple particle interference and error correction, Proc. Royal Society of London Series A. 452 (1996) 2551-2577.